Janek Schoffit *23. April 2018*

ITS Stoffsammlung

Gliederung

1 OSI Schichtenmodell **3**
1.1 Modell . . . 3

2 Protokollstack **3**

3 IP **4**
3.1 IPv4 . . . 4
3.1.1 Adressformat . . . 4
3.1.2 Netzklassen . . . 4
3.1.3 Classless Inter-Domain Routing (CIDR) . . . 5
3.2 IPv6 . . . 5
3.2.1 Gründe für IPv6 . . . 5
3.2.2 Struktur der Adressen und Begriffe . . . 5
3.2.3 Adressnotation . . . 5
3.2.4 URL-Notation . . . 5
3.2.5 Autokonfiguration (SLAAC) . . . 5

4 DHCP (Dynamic Host Configuration Protocol) **6**
4.1 DHCPv4 . . . 6
4.1.1 Manuelle Zuordnung (statisches DHCP) . . . 6
4.1.2 Automatische Zuordnung . . . 6
4.1.3 Dynamische Zuordnung . . . 6
4.1.4 Ports . . . 6
4.2 DHCPv6 . . . 6
4.2.1 Ports . . . 6

5 VLAN (Virtual Local Area Network) **7**
5.1 Vor- und Nachteile . . . 7
5.2 VLAN Typen . . . 7
5.3 Trunk . . . 7

6 Backup **8**
6.1 Sicherungsarten . . . 8
6.1.1 Großvater - Vater - Sohn Prinzip . . . 8
6.1.2 Vollbackup . . . 8
6.1.3 Inkrementelles Backup . . . 8
6.1.4 Differentielles Backup . . . 8
6.2 RAID . . . 9
6.2.1 RAID 0 (Striping) . . . 9
6.2.2 RAID 1 (Mirroring) . . . 9
6.2.3 RAID 5 (Block-Level-Striping + Parität) . . . 10
6.2.4 RAID 6 (Block-Level-Striping + doppelt verteilte Parität) . . . 10
6.2.5 RAID 01 . . . 10
6.2.6 RAID 10 . . . 11
6.2.7 RAID 50 . . . 11
6.3 Storage . . . 12

6.3.1 DAS (Direct Attached Storage) . . . 12
6.3.2 NAS (Network Attached Storage) . . . 12
6.3.3 SAN (Storage Area Network) . . . 12

7 DMZ (Demilitarized Zone) 13

8 Verschlüsselung 14
8.1 Hashfunktion . . . 14
8.1.1 Prüfsummen . . . 14
8.2 Symmetrische Verschlüsselung . . . 14
8.3 Asymmetrische Verschlüsselung . . . 14
8.3.1 Einfaches Beispiel . . . 14
8.3.2 RSA-Kryptosystem . . . 15
8.4 Hybride Verschlüsselung . . . 15
8.4.1 Einfaches Beispiel . . . 15

9 Netzwerkkabel Arten 16
9.1 Cat5 . . . 16
9.2 Cat5e . . . 16
9.3 Cat6 . . . 16
9.4 Cat7 . . . 16

10 Tunneling 17
10.1 IPSec (Internet Protocol Security) . . . 17
10.1.1 Authentisierung (AH) . . . 17
10.1.2 Verschlüsselung (ESP) . . . 17
10.1.3 Vergleich Transport- und Tunnelmodus . . . 18
10.2 VPN (Virtual Private Network) . . . 19
10.2.1 Netz zu Netz . . . 19
10.2.2 Client zu Netz . . . 19
10.3 SSH (Secure Shell) . . . 19
10.3.1 X Session . . . 19
10.3.2 Port Tunneling . . . 19
10.3.3 SCP . . . 19

1 OSI Schichtenmodell

Das OSI Schichtenmodell (Open Systems Interconnection Model) ist ein Referenzmodell für Netzwerkprotokolle.

1.1 Modell

#	OSI-Schicht	Beispiele	Kopplungselemente
7	Anwendungen (Application)	HTTP, FTP, SMTP, LDAP	Gateway, Proxy, Content-Switch
6	Darstellung (Presentation)	HTTP, FTP, SMTP, LDAP	Gateway, Proxy, Content-Switch
5	Sitzung (Session)	HTTP, FTP, SMTP, LDAP	Gateway, Proxy, Content-Switch
4	Transport (Transport)	TCP, UDP	Gateway, Proxy, Content-Switch
3	Vermittlung (Network)	ICMP, IP, IPsec	Router, Layer-3-Switch
2	Sicherung (Data Link)	Ethernet, Token Ring, MAC	Bridge, Layer-2-Switch
1	Bitübertragung (Physical)	Ethernet, Token Ring, MAC	Netzwerkkabel, Repeater, Hub

2 Protokollstack

3 IP

Das Internet Protocol ist die erste vom Übertragungsmedium unabhängige Schicht. Mithilfe von IP-Adresse und Subnetzmaske (Präfixlänge für IPv6) können Computer innerhalb eines Netzwerks logisch gruppiert werden.

3.1 IPv4

IPv4 is die erste Version des Internet Protocols, welche weltweit verbreitet und eingesetzt wurde, und bildet eine wichtige technische Grundlage des Internets.

3.1.1 Adressformat

Eine IPv4 Adresse besteht aus 4 dezimalen Zahlenblöcken bestehend aus jeweils 8 Bit (0-255). Mit 32 Bit können maximal $2^{32} = 4.294.967.296$ Adressen vergeben werden.

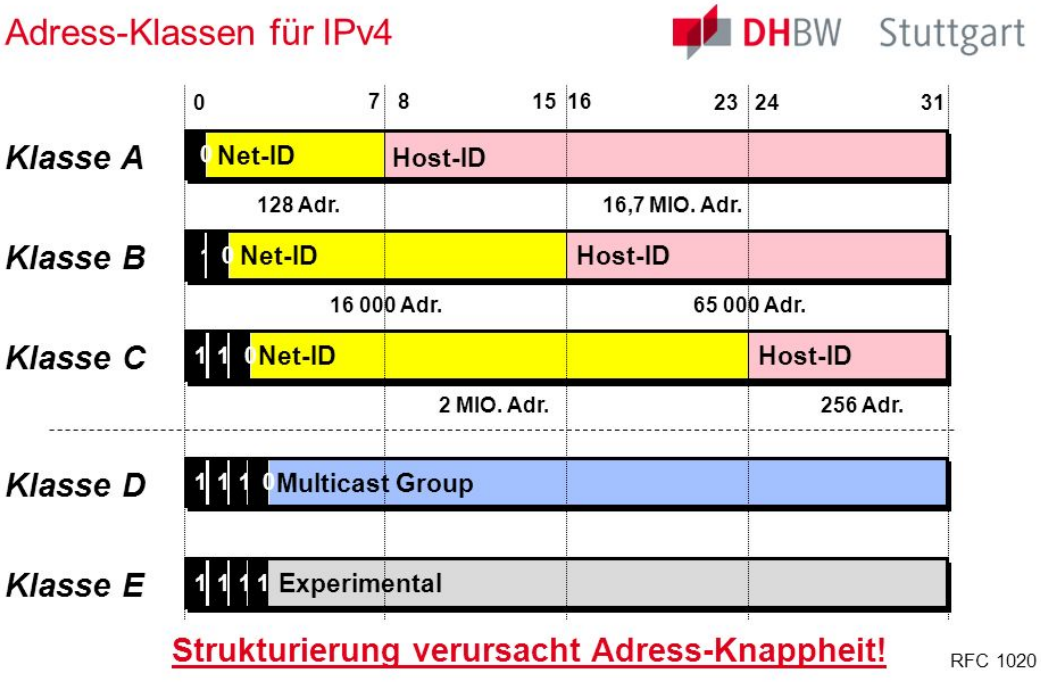
3.1.2 Netzklassen

Vor 1993 gab es fest vorgeschriebene Einteilungen für Netzwerkklassen mit einer festen Länge. Diese Einteilung ist sehr unflexibel, weshalb vorallem im WAN hauptsächlich das CIDR (Classless Inter-Domain Routing) Verfahren genutzt wird. Netzklassen werden jedoch immer noch häufig im lokalen Netz genutzt.

Die maximale Anzahl der zu vergebenen Host-Adressen in einem Netz ist:

$$2^{AnzahlBitsderHostadresse} - 2$$

Dabei wird die Netz- und Broadcastadresse abgezogen. Wenn nach max. Anzahl der PCs im Netz gefragt wird, sollte -3 gerechnet werden und damit das Gateway abgezogen werden.



3.1.3 Classless Inter-Domain Routing (CIDR)

3.2 IPv6

3.2.1 Gründe für IPv6

IPv4 verfügt über weniger Adressen wie es Menschen auf der Welt gibt. Da mittlerweile ein Großteil der Menschen über mindestens ein Netzwerkfähiges Gerät verfügen stößt IPv4 mit $2^{32} = 4.294.967.296$ an seine Grenzen.

3.2.2 Struktur der Adressen und Begriffe

Eine IPv6 besteht aus 128 Bit (8 Blöcke * 16 Bits) was theoretisch 2^128 Adressen entspricht. Die ersten 64 Bit bilden den Präfix, die letzten 64 Bit bilden einen für die Netzwerkschnittstelle eindeutigen Interface-Identifier. Eine Netzwerkschnittstelle kann unter mehreren IP-Adressen erreichbar sein mittels link-local Adressen und einer überall eindeutigen link-global Adresse. Derselbe Interface-Identifier kann damit Teil mehrerer IPv6 Adressen mit verschiedenen Präfixen sein. Diese können auch von verschiedenen ISPs kommen, was Multihoming vereinfacht. Der Interface-Identifier wird mit Hilfe der global eindeutigen MAC-Adresse erzeugt, wodurch die Nachverfolgung von Benutzern ermöglicht wird. Um dies aufzuheben wurden Privacy Extensions (PEX) entwickelt, welche den Interface-Identifier zufällig generieren und regelmäßig wechseln.

3.2.3 Adressnotation

- Blöcke werden Hexadezimal notiert ⇒ 16 Bit entsprechen 4 Hexadezimal Stellen
- Führende Nullen innerhalb eines Blocks dürfen ausgelassen werden: ?:0000:? ⇒ ?:0:?
- Mehrere Blöcke die 0 sind, dürfen zusammengefasst werden: ?:0:0:? ⇒ ?::? Diese Reduktion darf nur einmal gemacht werden
- Die letzten 4 Byte (der letzte Block) darf auch in herkömmlicher IPv4 Notation geschrieben werden: ::ffff:7f00:1 ⇒ alternative ::ffff:127.0.0.1 Diese Schreibweise wird vor allem bei Einbettung des IPv4-Adressraums verwendet

3.2.4 URL-Notation

In einer URL wird die IPv6 Adresse in eckige Klammern eingeschlossen, damit keine Verwechslung mit einer Portnummer entsteht:

http://[2001:0db8:85a3:08d3::0370:7344]:8080/

3.2.5 Autokonfiguration (SLAAC)

Mit Hilfe von Stateless Address Autoconfiguration (SLAAC, Zustandslose Adressenautokonfiguration) kann ein Host vollautomatisch eine Internetverbindung aufbauen. Dazu kommuniziert der Host mit dem nächstgelegenen Routern, um die notwendige Konfiguration zu ermitteln.

4 DHCP (Dynamic Host Configuration Protocol)

4.1 DHCPv4

DHCP ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. Es werden Informationen wie IP-Adresse, Netzmaske, Gateway, DNS und weiteres automatisch vergeben, soweit das vom Client Betriebssystem unterstützt wird. DHCP ist eine Erweiterung des Bootstrap-Protokolls (BOOTP), welches für Computer ohne eigene Festplatte notwendig war, wo sich der PC beim starten erst vom BOOTP-Server eine IP zuweisen ließ, um danach das Betriebssystem aus dem Netzwerk zu laden.

4.1.1 Manuelle Zuordnung (statisches DHCP)

In diesem Modus wird einer MAC-Adresse eine feste IP zugewiesen. Die Adressen werden auf unbestimmte Zeit zugeteilt. Dieses Konzept wird vorallem für Server-Dienste genutzt, die unter einer festen IP erreichbar sein sollen.

4.1.2 Automatische Zuordnung

In diesem Modus wird dem DHCP Server ein bestimmter IP Bereich vorgegeben, indem er Adressen automatisch vergeben darf. Die MAC-Adressen werden in einer Tabelle festgehalten und sind permanent. Das heißt, ein Gerät behält seine Adresse, auch wenn es zwischenzeitlich vom Netz getrennt wurde. Der Nachteil ist, dass neue Clients keine IP erhalten, wenn der gesamte Adressbereich vergeben ist, auch wenn die IP nicht mehr genutzt wird.

4.1.3 Dynamische Zuordnung

Dieser Modus verhält sich ähnlich wie die automatische Zuordnung. Jedoch gibt es eine Angabe, wielange eine Adresse verliehen werden darf (DHCP lease), bevor sich der Client wieder melden muss, um eine Verlängerung zu beantragen. Wenn er sich nicht meldet, wird die Adresse wieder frei.

4.1.4 Ports

DHCPv4 nutzt die UDP-Ports 68 (Client) und 67 (Server).

4.2 DHCPv6

IPv6 benötigt für die Adressvergabe keinen DHCP (siehe IPv6 Autokonfiguration). Der Host benötigt jedoch vom DHCP-Dienst eine Zuweisung für ein Gateway und einen DNS-Server. Sollten andere Konfigurationen benötigt werden, kann anstelle von der Autokonfiguration auch komplett DHCPv6 genutzt werden.

4.2.1 Ports

Abweichend zu DHCPv4 nutzt DHCPv6 die UDP-Ports 546 (Client) und 547 (Server).

5 VLAN (Virtual Local Area Network)

- logisches Teilnetz innerhalb eines Switches bzw. gesamten physischen Netzwerk
- Wird über IDs im Frame realisiert ?> Switch sorgt dafür, dass Datenpakete nicht in andere VLANs geleitet werden

5.1 Vor- und Nachteile

Vorteile:

- Priorisierung von Daten (z.B. bei VoIP VLAN)
- Broadcast Reichweite kann eingeschränkt werden
- Netze können besser gegen abhören abgesichert werden
- Firewalls auf Layer 3 Basis können eingesetzt werden

Nachteile:

- Switche sind deutlich teurer
- Bei dynamischen VLANs mit automatischem Lernmodus kann ein Gerät emuliert werden und dadurch in andere VLANs eindringen, wodurch diese unwirksam werden

5.2 VLAN Typen

Portbasiert Ein VLAN wird auf einen Port geschalten. Dadurch wird der Switch in mehrere logische Switches aufgeteilt. Wird eingesetzt, wenn mehr Übersicht benötigt wird und Ressourcenverbrauch vermieden werden muss.

Tagged Es werden Netzwerkpakete verwendet, die eine zusätzliche VLAN-Markierung tragen. Empfängt der Switch von einem älteren Endgerät Pakete ohne VLAN-Tag, muss er diesen Tag selbst anbringen.

Statisch Hier wird einem Port eines Switches fest eine VLAN-Konfiguration zugeordnet. Er gehört dann zu einem Port-basierten VLAN, zu einem untagged VLAN oder er ist ein Port, der zu mehreren VLANs gehört.

Dynamisch Bei der dynamischen Implementierung eines VLANs wird die Zugehörigkeit eines Frames zu einem VLAN anhand bestimmter Inhalte des Frames getroffen. Es wird bspw. anhand von MAC-, IP-Adressen oder Protokolltypen entschieden, welches VLAN das Gerät bekommt.

5.3 Trunk

VLAN-Trunks (VLT) werden genutzt, um mehrere VLANs über eine Leitung zur Verfügung zu stellen. Die einzelnen Ethernet-Frames bekommen dabei Tags angehängt, indem jeweils die VLAN-ID vermerkt ist. Dies wird bspw. beim verbinden von Switches benötigt, welche die gleichen VLANs haben (ansonsten müsste für jedes VLAN ein eigener Link gelegt werden) oder an Arbeitsplätzen, bei denen ein VoIP-Telefon und PC an einer Leitung angeschlossen wird. Trunks funktionieren auch mit Link Aggregation. VLAN Trunks sind unter IEEE 802.1Q standardisiert.

6 Backup

6.1 Sicherungsarten

6.1.1 Großvater - Vater - Sohn Prinzip

(auch Generationenprinzip genannt): Bei diesem Verfahren wird bspw. an 4 Tagen auf jeweils eine Festplatte (Sohn) das Backup geschrieben (Festplatten T1-T4). Am 5. Tag wird eine Wochensicherung gemacht und zurück gelegt (Festplatten W1-W4). Die darauffolgende Woche wird T1-T4 jeweils wieder mit neuen Backups überschrieben und eine neue Wochensicherung erzeugt. Am Ende des Monats wird die erste Monatssicherung erstellt (M1-M12). Daraufhin werden wieder alle T und W Festplatten überschrieben. Im neuen Jahr wird dann am Ende des 1. Monats zum ersten mal M1 überschrieben. Das heißt es können bis zu 1 Jahr alte Daten zurückgesichert werden.

6.1.2 Vollbackup

Hier werden alle Daten gesichert. Dies ist der Grundstein für andere Backupverfahren. Vorteil ist, es wird immer nur ein Band zur Wiederherstellung benötigt, jedoch hat das einen sehr hohen Speicherbedarf.

6.1.3 Inkrementelles Backup

Am ersten Tag wird ein Vollbackup erstellt. Daraufhin werden nurnoch die Unterschiede zum Vortag gesichert. Dieses Verfahren hat einen niedrigen Speicherbedarf, da immer nur Änderungen gespeichert werden und alle ungeänderten Daten in älteren Backups liegen. Die Wiederherstellung kann dadurch jedoch unter umständen zeitintensiv werden, da jede Datei in unterschiedlichen Inkrementen in der Vergangenheit liegen können und dadurch alle Speicher durchsucht werden müssen.

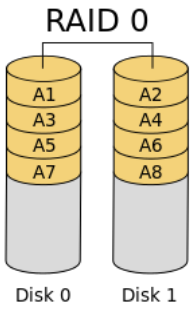
6.1.4 Differentielles Backup

Am ersten Tag wird ein Vollbackup erstellt. Daraufhin wird jeden Tag die Differenz (die Änderungen) zum Vollbackup gesichert. Der Vorteil dabei ist, dass nicht alle Bänder zur Verfügung stehen müssen, um etwas wiederherzustellen. Es reicht das Vollbackup + Tages Band. Dadurch ist die Rücksicherung auch schneller, benötigt jedoch mehr Speicherplatz wie das inkrementelle Backup.

6.2 RAID

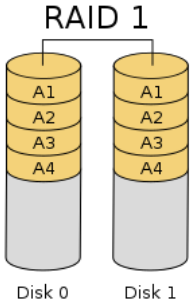
`RAID` steht für "Redundant Array of Independent Disks"

6.2.1 RAID 0 (Striping)



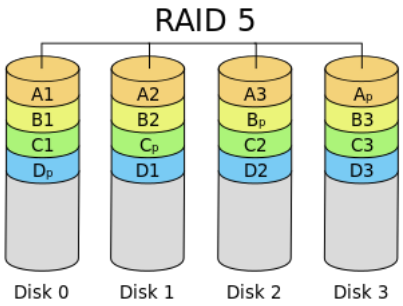
Es fehlt die Redundanz aber alle Festplatten werden zu einer logischen Platte zusammengeführt. Damit können Zugriffe auf allen Platten parallel (und nicht wie bei normalen Platten sequentiell) durchgeführt werden. Um mögclichst schnell Daten parallel abfragen zu können, werden diese in Datenblöcke zerlegt (striping) und auf den unterschiedlichen Platten verteilt. Die Größe der Datenblöcke wird als Striping-Granularität (auch chunk size) bezeichnet (meistens 64kB). Fällt eine Festplatte aus, können die Daten nicht mehr vollständig rekonstruiert werden (abgesehen von kleinen Dateien unter der chunk size des Systems).

6.2.2 RAID 1 (Mirroring)



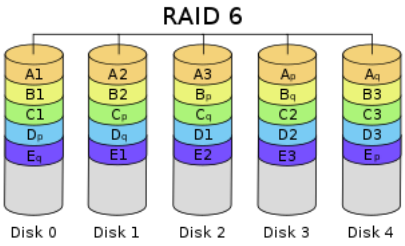
Hier werden alle Daten jeweils auf allen Festplatten gespeichert (gespiegelt). Dieses System bietet eine hohe Ausfallsicherheit, da bei einem Ausfall einer Platte die andere Festplatte immernoch alle Daten bereitstellen kann. Beim lesen der Daten wird die Leistung erhöht (bei 2 Platten doppelte Leseleistung), da parallel von verschiedenen Festplatten Sektoren gelesen werden kann (Geschwindigkeit gleich hoch wie bei RAID 0).

6.2.3 RAID 5 (Block-Level-Striping + Parität)



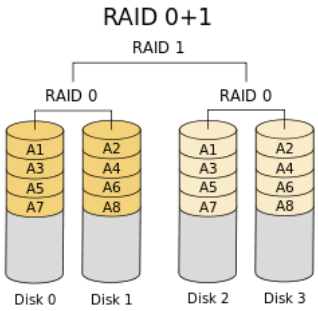
Hier werden die Daten wie bei RAID 0 in Blöcken verteilt auf die Festplatten, jedoch wird dazu immer eine Paritätsinformation erzeugt und auch auf den verschiedenen Platten gespeichert (Unterschied zu RAID 4). Dadurch können die Festplatten sehr Effizient genutzt werden und die Daten sind trotzdem redundant. Der Controller ist jedoch sehr teuer und lohnt sich bei wenigen Platten meistens nicht (RAID 10 günstiger). Die Parität wird durch eine XOR Operation über die Nutzdaten erstellt.

6.2.4 RAID 6 (Block-Level-Striping + doppelt verteilte Parität)



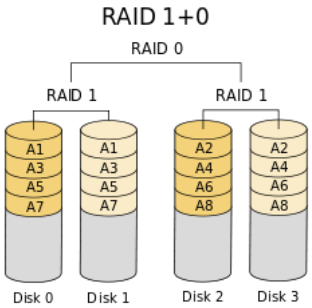
Dieses System verkraftet bis zu 2 gleichzeitig ausfallende Festplatten. Die Wiederherstellung einer Platte dauert viele Stunden in denen RAID 6 im Vergleich zu RAID 5 trotzdem noch vor einem weiteren Ausfall geschützt ist.

6.2.5 RAID 01



Ist ein RAID 1 Verbund über mehrere RAID 0 Verbünde (01 Leserichtung von unten nach oben). Dieser Verbund kann auch mit einer ungeraden Anzahl an Festplatten erzeugt werden (im Gegensatz zu RAID 10). Dann werden bei bspw. 3 Platten auf jeder 50% Nutzdaten und 50% Spiegelung der Nutzdaten einer anderen Platte eingeteilt. Die Daten werden wie bei RAID 0 gestriped und bei Ausfall müssen in diesem Fall 2 von 3 Platten in Takt sein, um die Daten vollständig wiederherstellen zu können.

6.2.6 RAID 10

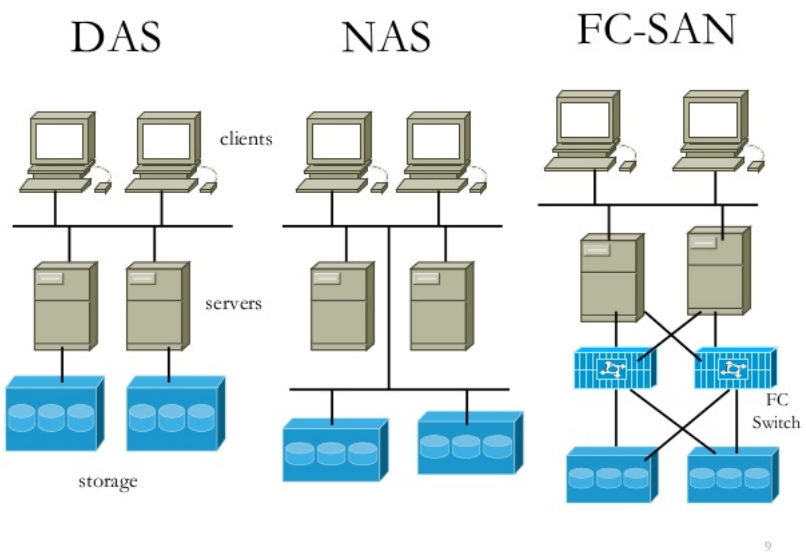


Ist ein RAID 0 Verbund über mehrere RAID 1 Verbünde. Dabei werden Sicherheit und gesteigerte Schreib-/Lesegeschwindigkeiten miteinander kombiniert. Hierbei wird immer eine gerade Anzahl >= 4 an Festplatten benötigt. Es bietet eine schnellere Rekonstruktion der Daten, da diese im unteren Zweig (RAID 1) wiederhergestellt werden und nicht über den Hauptzweig wie bei RAID 01.

6.2.7 RAID 50

Benötigt mindestens 6 Festplatten und bietet einen hohen Datendurchsatz, da die Daten auf 2 XOR-Units verteilt wird. Dieser Verbund wird bei Datenbanken verwendet, bei denen Schreibdurchsatz und Redundanz im Vordergrund stehen.

6.3 Storage



6.3.1 DAS (Direct Attached Storage)

An einen einzelnen Rechner angeschlossene Festplatten. Es kann nur über den Host auf die Festplatten zugegriffen werden. Sollte dieser also ausfallen, gibt es keinen Zugriff mehr auf die Daten. Ein Vorteil ist der geringe Hardwareaufwand, da die Platte nur mit einem PC verbunden werden muss und nicht weiter konfiguriert wird.

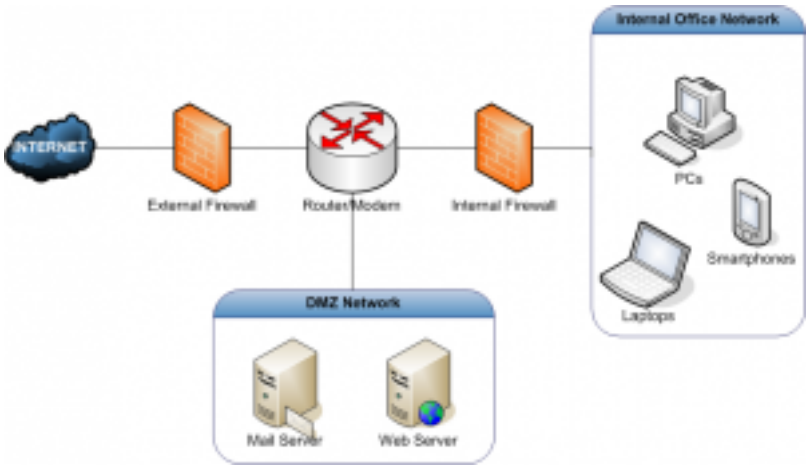
6.3.2 NAS (Network Attached Storage)

Ist ein einfach zu verwaltender Dateiserver. Es dient dazu die Speicherkapität im Netz freizugeben und muss daher über zusätzliche Übertragungsprotokolle (SMB/CIFS) verfügen. Vorteile dieses Systems sind: ein niedrigerer Energieverbrauch wie herkömmliche PC-Systeme. NAS können große Datenmengen mehreren Benutzern über Freigaben schnell zugänglich gemacht werden. NAS-Systeme können mit mehreren Festplatten ausgestattet werden und damit im RAID geschalten werden.

6.3.3 SAN (Storage Area Network)

Ist ein Netzwerk zur Anbindung von Disk-Arrays und Tape-Libraries an Server Systeme. Das bedeutet, Server belasten mit Zugriffen auf Daten nicht das interne Netzwerk, sondern können über Fibre Channel auf das SAN zugreifen. Die Zugriffe auf das Speichergerät und dessen Dateisystem wird durch den zugreifenden Rechner verwaltet (wie bei DAS). Strukturell ist ein SAN analog zu einem LAN aufgebaut ?> Router, Switches, Hubs

7 DMZ (Demilitarized Zone)



Die DMZ wird gegen andere Netze mit einer oder mehreren Firewalls abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentliche Dienste wie Email oder WWW ermöglicht werden und gleichzeitig ist das interne Netz vor äußeren Zugriffen geschützt. Bei einer Firewall muss diese über 3 Netzanschlüsse verfügen (WAN, DMZ, LAN). Im Falle von zwei Firewalls, wird die erste an der WAN Seite positioniert und mit einem Switch vebunden, welcher dann zur DMZ und zur zweiten Firewall (zum LAN) leitet. Ein Verbindungsaufbau sollte immer aus dem LAN in die DMZ erfolgen und nicht andersrum.

8 Verschlüsselung

8.1 Hashfunktion

Eine Hashfunktion dient im allgemeinen dazu eine große Eingabemenge in auf einer kleineren Zielmenge eindeutig abzubilden. Die Eingabemenge kann Elemente unterschiedlicher Länge enthalten, die Elemente der Zielmenge haben hingegen normalerweise eine feste Länge. Eine gute Hashfunktion sollte für Eingaben möglichst wenige Kollisionen erzeugen. Eine Kollision tritt dann auf, wenn unterschiedliche Eingaben den selben Hash zurück liefern. Aus einem Hash kann nicht die Eingabemenge zurück errechnet werden.

8.1.1 Prüfsummen

Eine Prüfsumme ist ein Hash mit dem bspw. Integrität von Daten überprüft werden kann. Prüfsummen werden bei der Datenübertragung oder der Datensicherung verwendet. Mit Prüfsummen ist es bspw. möglich Bitfehler in einer Datei zu erkennen, indem von der Originaldatei ein Hash erstellt wird und dieser mit dem Hash der Datei zu einem späteren Zeitpunkt verglichen wird.
Beispiele für bekannte kryptografische Hashfunktionen:

MD5 Message-Digest Algorithm 5 (Gilt nicht mehr als sicher)

SHA Secure Hash Algorithm

8.2 Symmetrische Verschlüsselung

Bei dieser Methode wird ein Schlüssel zur Ver- und Entschlüsselung genutzt. Dieser wird zuerst ausgetauscht und danach die verschlüsselten Daten gesendet. Hierbei besteht das Risiko, dass der Schlüssel beim Austausch abgefangen wird.

8.3 Asymmetrische Verschlüsselung

Bei dieser Methode gibt es zwei Schlüssel. Ein Verschlüsselungs-Schlüssel (Public Key) und ein Entschlüsselungs-Schlüssel (Private Key). Der öffentliche Schlüssel ist jedem bekannt und muss nicht über einen sicheren Weg ausgetauscht werden, da dieser Schlüssel nur zum verschlüsseln genutzt werden kann. Dieses Verfahren ist deutlich langsamer (RSA ist ca. 1000x langsamer wie DES). Mit diesem Verfahren können auch Texte digital signiert werden. Damit kann dann sichergestellt werden, dass die angegebene Person auch tatsächlich den Text geschrieben hat. Der Text bleibt dabei weiterhin im Klartext, jedoch wird über den Text ein Hash gebildet und dieser mit dem privaten Schlüssel verschlüsselt. Beim validieren, wird mit dem Public Key festgestellt, ob die Nachricht vom angegebenen Autor verfasst wurde und mit dem Hash geprüft, ob der Text verändert wurde.

8.3.1 Einfaches Beispiel

A will Daten an B senden

1. A verschlüsselt mit dem public key von B
2. B entschlüsselt mit dem private key (von B)

8.3.2 RSA-Kryptosystem

Dieses Verfahren kann sowohl zum verschlüsseln als auch zum digitalen signieren verwendet werden. Es wurde 1977 als erstes asymmetrische Verschlüsselungsverfahren erfunden, welches 1983 patentiert wurde. Die Abkürzung RSA steht für die Familiennamen der Erfinder Rivest, Shamir und Adleman.

8.4 Hybride Verschlüsselung

Bei dieser Methode werden die Vorteile der symmetrischen und asymmetrischen Verschlüsselung vereint. Die asymmetrische Verschlüsselung wird zum Verbindungsaufbau genutzt, um über diese Verbindung einen Session Key auszutauschen, welcher dann symmetrisch für die Nutzdaten verwendet wird. Dieses Verfahren wird bspw. bei HTTPS verwendet.

8.4.1 Einfaches Beispiel

A will Daten an B senden

1. A generiert session key
2. A verschlüsselt den session key mit dem public key von B
3. B entschlüsselt den session key mit dem private key (von B)
4. Datenübertragung wird nun mit dem symmetrischen session key ver- und entschlüsselt

9 Netzwerkkabel Arten

9.1 Cat5

9.2 Cat5e

9.3 Cat6

9.4 Cat7

10 Tunneling

Beim Tunneling mit Hilfe von Datenpaketkapselung ein virtueller Tunnel erstellt, der über das Internet bzw. ein fremdes Netzwerk verbunden ist. Dadurch wird es bspw. möglich private LANs miteinander über das Internet zu verbinden oder sich auf einen Rechner zu schalten.

10.1 IPSec (Internet Protocol Security)

IPSec ist ein Protokollstapel der eine gesicherte Kommunikation über das potentiell unsichere Internet ermöglicht. IPSec arbeitet auf der Vermittlungsschicht, um eine Verschlüsselung auf Netzwerkebene bereitzustellen.
Es beinhaltet vier wichtige Sicherheitsfunktionen:

1. Verschlüsselung - um mitlesen zu verhindern
2. Authentisierung der Nachricht - zum sicherstellen, dass die Pakete unverfälscht sind (Paketintegrität)
3. Authentisierung des Absenders - zur unzweifelhaften Zuordnung eines Senders/Empfängers (Paketauthentizität)
4. Verwaltung von Schlüsseln

10.1.1 Authentisierung (AH)

Der Authentication Header (AH) sorgt für die Authentisierung und Integrität der zu übertragenden Pakete und Protokollinformationen. Der äußere IP-Header wird für die Integritätsprüfung mit gehasht, wodurch auf AH-Header keine Art von NAT anwendbar ist. Im AH-Paket befindet neben anderen Feldern ein Security Profile Index (SPI) und eine Sequenznummer. Diese Sequenznummer wird zum Schutz vor Replay-Attacks verwendet werden. Das heißt ein Paket kann nicht von dritten aufgezeichnet werden und zur wiederholten Authentifizierung mit gefälschter Identität verwendet werden.

10.1.2 Verschlüsselung (ESP)

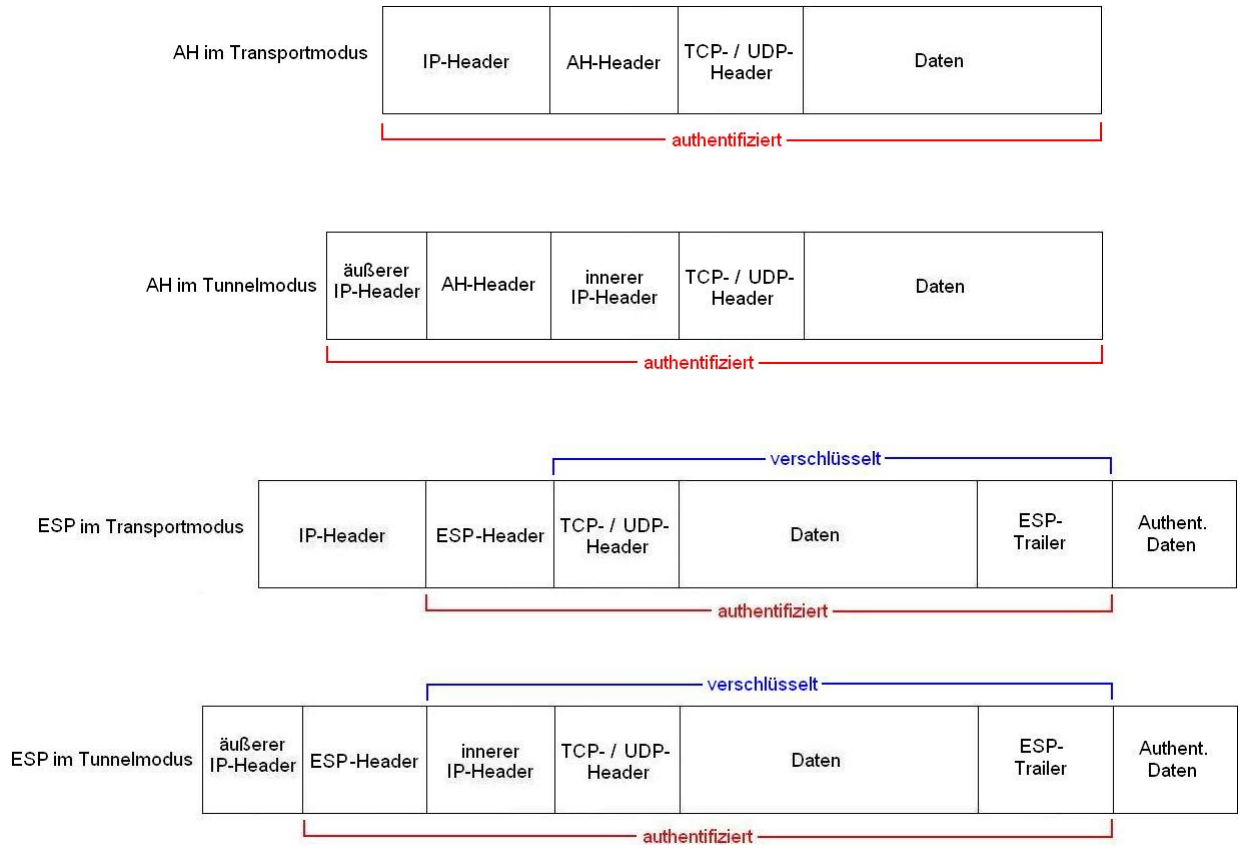
Die Verschlüsselung erfolgt über ESP (Encapsulating Security Payload), welches durch Hashing-Verfahren auch direkt die Integrität des Datenpakets sicherstellt. Zur Verschlüsselung der Nutzdaten können beliebige Verschlüsselungsverfahren eingesetzt werden.

10.1.3 Vergleich Transport- und Tunnelmodus

Der Transportmodus verbindet verbindet zwei Endpunkte direkt miteinander (Peer-to-Peer) z.B. über auf den Geräten installierte Software.
Im Tunnelmodus werden zwei IP-Netze miteinander verbunden. Die Endpunkte werden dabei von zwei Routern bzw. VPN-Gateways gebildet.

`IPSec im Transportmodus`: In diesem Modus wird der IPSec-Header zwischen dem IP-Header und den Nutzdaten eingefügt. Der IP-Header bleibt unverändert/unverschlüsselt und dient zum Routing des Pakets vom Sender zum Empfänger. Beim Empfang werden die ursprünglichen Nutzdaten (TCP-/UDP-Pakete) ausgepackt und an die höherliegende (OSI-)Schicht weitergegeben.

`IPSec im Tunnelmodus`: Hier wird das ursprüngliche Paket komplett gekapselt und ein neuer äußerer IP-Header hinzugefügt, um das Routing zum jeweiligen Endpunkt zu ermöglichen. Der innere IP-Header wird für das hinter dem Gateway des Endpunktes befindlichen Netz verwendet. Im Tunnelmodus sind Gateway-zu-Gateway- oder auch Peer-zu-Gateway-Verbindungen möglich. Ein Vorteil des Tunnelmodus ist, dass nur zwischen den Gateways IPSec implementiert werden muss. Angreifer können dadurch nur die Tunnelendpunkte festellen, jedoch nicht den gesamten Weg von den dahinter liegenden Clients.



10.2 VPN (Virtual Private Network)

10.2.1 Netz zu Netz

10.2.2 Client zu Netz

10.3 SSH (Secure Shell)

10.3.1 X Session

10.3.2 Port Tunneling

10.3.3 SCP